CybelAngel | A LEADING ETI PLATFORM

Understand how CybelAngel is compliant with DORA and NIS 2

CybelAngel's unified platform integrates our advanced services and expertise with leading cybersecurity frameworks and regulations, including NIST CSF 2.0, the EU Digital Operational Resilience Act (DORA), and the NIS 2 Directive We empower organizations to achieve and maintain a robust security posture.

NIST CSF 2.0

The NIST Cybersecurity Framework 2.0 provides a comprehensive and adaptable structure for managing cybersecurity risks. Its six core functions—Govern, Identify, Protect, Detect, Respond, and Recover—offer a clear roadmap for organizations of all sizes and sectors. By aligning with NIST CSF 2.0, companies can improve their risk management, enhance compliance with various standards (like GDPR, HIPAA, ISO), and build resilience against cyber threats. CybelAngel's platform directly supports the implementation of NIST CSF 2.0 by providing external risk visibility and actionable threat intelligence across each of these functions.

DORA (Digital Operational Resilience Act)

DORA aims to strengthen the digital operational resilience of the financial sector in the EU. It mandates that financial entities implement robust ICT risk management frameworks, conduct regular resilience testing, and establish incident reporting mechanisms. CybelAngel's external risk monitoring capabilities provide critical visibility into third-party risks and vulnerabilities, enabling financial institutions to meet DORA's requirements for supply chain security and incident detection.

NIS 2 Directive

The NIS 2 Directive expands the scope of cybersecurity regulations to a wider range of critical sectors across the EU. It sets out minimum cybersecurity standards and incident reporting obligations for essential and important entities. CybelAngel's proactive threat detection and vulnerability management capabilities help organizations comply with NIS 2 by identifying and mitigating cyber risks before they can impact essential services.

How to leverage CybelAngel to maximise NIS 2 and DORA Compliance

Compliance Goal / Regulatory Requirement	Clarified Contribution	CybelAngel Modules
Comprehensive ICT Asset Inventory & Exposure Visibility DORA Art. 5(1)(c); NIS2 Art. 21(2)(b)	Identifies exposed Shadow IT, IoT, RDP, cloud assets, and their vulnerabilities;	Attack Surface Management
External Credential Leak Monitoring & Access Control DORA Art. 6; NIS2 Art. 21(2)(c)	Detects leaked credentials on open/dark web; supports internal IAM enforcement	Credential Intelligence
Sensitive Data Protection & Data Loss Prevention DORA Art. 5(1)(d); NIS2 Art. 21(2)(d); GDPR Art. 32	Detects exposed sensitive data in cloud, S3 buckets, and databases; complements encryption and access controls	Data Breach Prevention
Threat Intelligence & Early Warning DORA RTS (Threat Intelligence); NIS2 ID.RA-3	Provides actionable external threat insights, including threat actor activity and ransomware trends	Threat Intelligence Dark Web Monitoring
Phishing & Impersonation Detection DORA Art. 5(1)(e); NIS2 Art. 21(2)(e)	Detects phishing attempts, fraudulent and impersonation domains; strengthens incident detection	Domain Protection
API Security & Vulnerability Management DORA Art. 5(1)(d); NIS2 Art. 21(2)(b,d)	Identifies unsecured or unknown APIs exposed to the internet; supports attack surface discovery and risk reduction	API Exposure Monitoring
Brand Protection & Executive Impersonation (Indirectly related to DORA/NIS2 reputation and phishing response)	Detects fake brand or personnel profiles on social media; supports brand protection and executive impersonation detection	Social Media Impersonation
Third-Party Risk Assessment & Due Diligence DORA Art. 28; NIS2 Art. 21(2)(f)	Assesses compliance and cyber resilience of key third-party providers through EASM and due diligence	Third Party Assessment / Due Diligence

CybelAngel